OIPE
MAY 26 2006
IAP43
PATENT & TRADEMARK OFFICE

Attorney's Docket No.: 12221-010001

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Massimiliano Antonio Poletto et al. Art Unit : 2184
Serial No. : 10/066,232 Examiner : Perungavoor, Venkatanaray
Filed : January 31, 2002
Title : DENIAL OF SERVICE ATTACKS CHARACTERIZATION

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF ON BEHALF OF MASSIMILIANO ANTONIO POLETTO ET AL.

The Appeal Brief fee is enclosed. Please apply any other charges or credits to Deposit Account No. 06-1050.

05/26/2006 SDENBOB1 00000062 10066232
01 FC:2402 250.00 OP

CERTIFICATE OF MAILING BY FIRST CLASS MAIL

I hereby certify under 37 CFR §1.8(a) that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage on the date indicated below and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

May 23, 2006
Date of Deposit

Marie Collins
Signature

Marie Collins
Typed or Printed Name of Person Signing Certificate

(i.) Real Party In Interest

The real party in interest in the above application is Mazu Networks, Inc.

(ii.) Related Appeals and Interferences

The appellant is not aware of any appeals or interferences related to the above-identified patent application.

(iii.) Status of Claims

This is an appeal from the decision of the Primary Examiner in an Office Action dated November 11, 2005, finally rejecting claims 1-7, 18-22, and 28-37. The examiner indicated that claims 8-17, 22-24 and 39-40 were objected to as containing allowable subject matter but being dependent on a rejected base claim. The claims have been twice rejected. Claims 1-7, 18-22, and 28-37 are the subject of this appeal.

(iv.) Status of Amendments

All amendments have been entered. Appellant filed a Request for Reconsideration and a Notice of Appeal on February 7, 2006.

(v.) Summary of Claimed Subject Matter

Background

The invention relates to techniques to thwart network-related denial of service attacks.

In denial of service attacks, an attacker sends a large volume of malicious traffic to a victim in an attempt to prevent the victim from responding to legitimate traffic.

Appellant's Invention

Claim 1

One aspect of Appellant's invention is set out in claim 1, as a process that monitors network traffic through a monitoring device "The gateway 26 devices are located at the edges of the Internet 14, for instance, at the entry points of data centers. The gateway devices constantly

analyze traffic, looking for congestion or traffic levels that indicate the onset of a DoS attack." [Specification page 5, lines 23-27] disposed between a data center and a network for thwarting denial of service attacks on the data center. "The victim 12 is coupled to the Internet 14 or other network. For example, the victim 12 has a web server located at a data center (not shown)." [Specification page 4, lines 30-32].

Inventive features of claim 1 include a detection process to determine if the values of a parameter of network traffic exceed normal values for the parameter to indicate an attack on the data center. "Several methods can be used separately or in combination to detect, malicious traffic flows. For example, the gateway 26 can detect DoS attacks using at least one or more of the following methods including:" [Specification page 17, lines 23-26].

Inventive features of claim 1 also a characterization process to build a histogram for the parameter to compute significant outliers in a parameter and classify the attack. "Referring to FIG. 12, attack characterization 139 is based on comparison of historical histogram data with near-real-time histogram data for one or several parameters (e.g., source/dest IP address, source/dest TCP/UDP ports, IP protocol, IP TTL, IP length, hash of payload fragment; IP TOS field and TCP flags). [Specification page 25, lines 23-29].

Typically, historical histograms are based on time periods that can range from 1 hour to 1 week. During an attack, attack histograms are produced 142 for time periods, e.g., in the 10-300sec range. For each parameter, the two histograms are normalized 144 (integral set equal to 1) and their difference 146 is used to compute 148 significant outliers." [Specification page 25, line 29 to page 26, line 3].

Inventive features of claim 1 also include a filtering process for filtering of network packets based on the characterization process. "The attack characterization process 139 correlates 150 the suspicious parameters and determines existence of correlations of those parameters that can be indications of attacks. If under attack 152 the process 139 will employ filtering." [Specification page 26, lines 19-23].

Claim 7

Claim 7 claims a method for thwarting denial of service attacks on a data center. This feature generally finds support at least as the analogous feature of claim 1.

Inventive features of claim 7 include producing a histogram of received network traffic for at least one parameter of network packets. This feature generally finds support at least as the analogous feature of claim 1.

Inventive features of claim 7 also include characterizing an attack based on comparison of a historical histogram with the produced histogram data for one or more parameters. This feature generally finds support at least as the analogous feature of claim 1.

Claim 21

Claim 21 claims a monitoring device for thwarting denial of service attacks on a data center. "Another alternate implementation could combine thresholds with a histogram analysis, and trigger traffic characterization whenever a histogram for some parameter differed significantly (by uniformity test, or for example, by subtracting normalized histograms) from the historical histogram. [Specification page 19, lines 10-15]. ... Optionally, the gateway 26 executing the detection process 131 can build 134 a histogram ... for any attribute or function of an attribute of network packets to use in determining if an attack is occurring." [Specification page 25, lines 12-16].

Inventive features of claim 21 include a computing device executing a process to build at least one histogram for at least one parameter of network traffic. This feature generally finds support at least as the analogous feature of claim 1.

Inventive features of claim 21 also include a process to characterize an attack based on a comparison of a historical histogram of the at least one parameter to the built at least one histogram for the at least one parameter. This feature generally finds support at least as the analogous feature of claim 1.

Claim 28

Claim 28 claims a computer program product residing on a computer readable medium. "The gateway 26 comprises a software program executing on a device, e.g., a computer 27 that is disposed at the edge of the data center 20 behind an edge router coupled in the Internet 14." [Specification page 6, lines 26-28].

Inventive features of claim 28 include instructions to build a histogram for a parameter of network traffic. This feature generally finds support at least as the analogous feature of claim 1.

Inventive features of claim 28 also include instructions to use the histogram data for the parameter to characterize an attack. This feature generally finds support at least as the analogous feature of claim 1.

Claim 32

Claim 32 claims a method of protecting a data center during a denial of service attack. This feature generally finds support at least as the analogous feature of claim 1.

Inventive features of claim 32 include monitoring network traffic through a gateway disposed between the data center and a network. "During normal operation, the gateway collects 132 information about normal network traffic for these parameters. The gateway determines 137 normal or reasonable values for each of the attributes or functions of attributes that the gateway tracks, as mentioned above. The detection process 131 uses some statistic about the flow, such as an average of a traffic ratio of the standard deviation to a mean of a histogram attribute over a time window, e.g., over a minute, or hour, etc." [Specification page 24, lines 10-18.

Inventive features of claim 32 also include determining if values of at least one parameter exceed normal, threshold values expected for the parameter to indicate an attack on the site. "The gateway determines 137 normal or reasonable values for each of the attributes or functions of attributes that the gateway tracks, as mentioned above." [Specification page 24, lines 12-14].

Inventive features of claim 32 also include producing a histogram for the at least one parameter of network traffic to characterize the attack by comparing the histogram to at least one historical histogram for that parameter. "Consider a historical histogram H, and a current (under attack) histogram C. The use of the noise reduction process 151 is to normalize each histogram so the integral of each histogram equals one. Then for each bucket i component of the histogram, the noise reduction process computes a difference value D_i ($D_i = C_i - H_i$) to determine a difference value for each bucket relative to historical norm, and produces a "difference histogram," D as generally described above to find outliers." [Specification page 27, line 5-13].

Inventive features of claim 32 also include filtering out traffic based on characterizing the traffic, which the gateway deems to be part of an attack. This feature generally finds support at least as the analogous feature of claim 1.

Claim 37

Claim 37 is directed to a method to reduce blocking of legitimate traffic in a process to protect a victim site during a denial of service attack. This feature generally finds support at least as the analogous feature of claim 1.

Inventive features of claim 37 include producing a histogram of network traffic to characterize an attack. This feature generally finds support at least as the analogous feature of claim 1. This feature generally finds support at least as the analogous feature of claim 1.

Inventive features of claim 37 also include filtering out traffic deemed part of an attack. This feature generally finds support at least as the analogous feature of claim 1. "Referring to FIG. 14, a second filtering mechanism is aggregate filtering 170. Aggregate filtering 170 allows constant-time filtering, independent of the number of individual parameter values used for filtering. Based on the correlation histogram, the process 170 constructs 172 a master correlation vector (a bit vector that has 1-bits corresponding to the most important parameter correlations)." [Specification page 29, lines 26-32].

Inventive features of claim 37 also include constructing a master correlation vector having asserted bits corresponding to the most important parameter correlations. "Based on the correlation histogram, the process 170 constructs 172 a master correlation vector (a bit vector that has 1-bits corresponding to the most important parameter correlations)." [Specification page 29, lines 29-31].

Inventive features of claim 37 also include initializing a packet's correlation bit vector to 0, and for every parameter: "Given a packet, the process initializes 174 the packet's correlation bit vector to 0. The process 170 loops for every parameter (TTL, etc.), and retrieves 176 the parameter in the parameter suspicious vector to construct 178 the packet' correlation bit vector. If the bit in the suspicious vector is 1, the process sets the relevant bit in the packet's correlation vector to a 1 (in the example, bit 0 for TTL, 1 for source address, 2 for dest address)." [Specification page 30, lines 4-12].

Inventive features of claim 37 also include retrieving the parameter in a parameter suspicious vector to construct the packet' correlation bit vector. "In the example above, since buckets 4 and 5 were deemed suspicious, the master correlation bit vector would be 00110000 (bits 4 and 5, decimal 48)." [Specification page 30, lines 1-3].

Inventive features of claim 37 also include using the value of the packet's correlation bit vector to index into the master correlation bit vector. "The process uses 180 the value of the packet's correlation bit vector to index into the master correlation bit vector. The process 170 tests 182 the indexed bit in the master correlation vector. If the bit in the master correlation bit vector is a one, the packet is dropped, otherwise the packet is forwarded."[Specification page 30, line 13-18].

(vi.) Grounds of Rejection to be Reviewed on Appeal

1. Claims 7, 21, and 22 stand rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,304,262 Maloney et al. (hereinafter Maloney).

2. Claims 1-6, 18-20, 22, and 28-37 stand rejected under 35 U.S.C. 103(a), as being unpatentable over U.S. Patent 6,301,668 B1 Gleichauf et al. (hereinafter Gleichauf) in view of Maloney.

(vii.) Argument

Anticipation

"It is well settled that anticipation under 35 U.S.C. §102 requires the presence in a single reference of all of the elements of a claimed invention." *Ex parte Chopra*, 229 U.S.P.Q. 230, 231 (BPA&I 1985) and cases cited.

"Anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim." *Connell v. Sears, Roebuck & Co.*, 220 U.S.P.Q. 193, 198 (Fed. Cir. 1983).

"This court has repeatedly stated that the defense of lack of novelty (i.e., 'anticipation') can only be established by a single prior art reference which discloses each and every element of the claimed invention." *Structural Rubber Prod. Co. v. Park Rubber Co.*, 223 U.S.P.Q. 1264, 1270 (Fed. Cir. 1984), citing five prior Federal Circuit decisions since 1983 including *Connell.*

In a later analogous case the Court of Appeals for the Federal Circuit again applied this rule in reversing a denial of a motion for judgment n.o.v. after a jury finding that claims were anticipated. *Jamesbury Corp. v. Litton Industrial Prod., Inc.*, 225 U.S.P.Q. 253 (Fed. Cir. 1985).

After quoting from *Connell*, "Anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim," 225 U.S.P.Q. at 256, the court observed that the patentee accomplished a constant tight contact in a ball valve by a lip on the seal or ring which interferes with the placement of the ball. The lip protruded into the area where the ball will be placed and was thus deflected after the ball was assembled into the valve. Because of this constant pressure, the patented valve was described as providing a particularly good seal when regulating a low pressure stream. The court quoted with approval from a 1967 Court of Claims decision adopting the opinion of then Commissioner and later Judge Donald E. Lane:

> [T]he term "engaging the ball" recited in claims 7 and 8 means that the lip contacts the ball with sufficient force to provide a fluid tight seal ****. The Saunders flange or lip only sealingly engages the ball 1 on the upstream side when the fluid pressure forces the lip against the ball and never sealingly engages the ball on the downstream side because there is no fluid pressure there to force the lip against the ball. The Saunders sealing ring provides a compression type of seal which depends upon the ball pressing into the material of the ring. *** The seal of Saunders depends primarily on the contact between the ball and the body of the sealing ring, and the flange or lip sealingly contacts the ball on the upstream side when the fluid pressure increases. 225 U.S.P.Q. at 258.

Relying on *Jamesbury*, the ITC said, "Anticipation requires looking at a reference, and comparing the disclosure of the reference with the claims of the patent in suit. A claimed device is anticipated if a single prior art reference discloses all the elements of the claimed invention as arranged in the claim." *In re Certain Floppy Disk Drives and Components Thereof*, 227 U.S.P.Q. 982, 985 (U.S. ITC 1985).

Obviousness

"It is well established that the burden is on the PTO to establish a prima facie showing of obviousness, *In re Fritsch*, 972 F.2d. 1260, 23 U.S.P.Q.2d 1780 (C.C.P.A., 1972)."

"It is well established that there must be some logical reason apparent from the evidence or record to justify combination or modification of references. *In re Regal*, 526 F.2d 1399 188,

U.S.P.Q.2d 136 (C.C.P.A. 1975). In addition, even if all of the elements of claims are disclosed in various prior art references, the claimed invention taken as a whole cannot be said to be obvious without some reason given in the prior art why one of ordinary skill in the art would have been prompted to combine the teachings of the references to arrive at the claimed invention. Id. Even if the cited references show the various elements suggested by the Examiner in order to support a conclusion that it would have been obvious to combine the cited references, the references must either expressly or impliedly suggest the claimed combination or the Examiner must present a convincing line of reasoning as to why one skilled in the art would have found the claimed invention obvious in light of the teachings of the references. *Ex Parte Clapp*, 227 U.S.P.Q.2d 972, 973 (Board. Pat. App. & Inf. 985)."

"The mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification." *In re Gordon*, 221 U.S.P.Q. 1125, 1127 (Fed. Cir. 1984).

> Although the Commissioner suggests that [the structure in the primary prior art reference] could readily be modified to form the [claimed] structure, "[t]he mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification." *In re Laskowski*, 10 U.S.P.Q. 2d 1397, 1398 (Fed. Cir. 1989).

"The claimed invention must be considered as a whole, and the question is whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination." *Lindemann Maschinenfabrik GMBH v. American Hoist & Derrick*, 221 U.S.P.Q. 481, 488 (Fed. Cir. 1984).

> Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination. Under Section 103, teachings of references can be combined only if there is some suggestion or incentive to do so. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984) (emphasis in original, footnotes omitted).

"The critical inquiry is whether 'there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination.'" *Fromson v. Advance Offset Plate, Inc.*, 225 U.S.P.Q. 26, 31 (Fed. Cir. 1985).

1. Claims 7, 21, and 22 are not anticipated by U.S. Patent 6,304,262 to Maloney et al.

Claims 7 and 21

For the purposes of this appeal only Claims 7 and 21 stand or fall together. Claim 7 is representative of this group of claims.

Claim 7 is directed to a method for thwarting denial of service attacks on a data center. Claim 7 is neither anticipated nor obvious over Maloney, since Maloney neither describes nor suggests at least the feature of producing a histogram of received network traffic for at least one parameter of network packets and characterizing an attack based on comparison of a historical histogram with the produced histogram data for one or more parameters.

The examiner contends that: ""Maloney discloses the building of graph and the classifying of the attack see Col 10 Ln 37-45 & Col 6 Ln 64-Col 7 Ln 6."

Appellant contends that Maloney fails to disclose at Col. 10, lines 37-45 and Col. 6, line 64 to Col 7, line 6 or elsewhere the features of claim 7. At Col. 10, lines 37-45, Maloney discloses:

> **Data stored in a flat text file by operation of the discovery tool 12 is utilized by the KB summation tool of the knowledge base tool set 96 to create a statistical matrix of the data contained in packet and session logs. For example, the instance of a protocol may be used as the Y access and the source IP address may be used as the X access. After selection of the packet or session log has been made, the KB summation tool screens the appropriate log file and displays available access criteria to create a graph. In the analysis of a typical network, a large number of files will be generated. The file manipulation tool of the knowledge base tool set 96 provides an interface to reduce the volume of generated files that must be sorted through. It enables files to be deleted or moved based on the file size, type, or contents for purposes of enhancing subsequent processing. Generated files are processed according to a chosen criteria for all files in a group.**

Maloney does not disclose a histogram. Moreover, Appellant contends that were Maloney's teachings be construed to define a histogram, Maloney still fails to describe "characterizing an attack based on comparison of a historical histogram with the produced

histogram data for one or more parameters." At Col. 10, lines 37-45, Maloney discloses that the KB summation tool creates a statistical matrix of the data contained in packet and session logs. "For example, the instance of a protocol may be used as the Y access and the source IP address may be used as the X access." This disclosure does not describe what one would consider to be a histogram, as used in claim 7. Maloney however states that: "the KB summation tool screens the appropriate log file and displays available access criteria to create a graph." At Col. 6, line 64 to Col 7, line 6 Maloney discloses:

> **Following parsing of the knowledge base 16 the analytical engine 20 responds to the data for preparation and converting into vector-based nodal diagrams. Typically the analytical engine 20 creates associations between a number of different charts to determine if such data charts correlate or differentiate. Relationships between an array of data sources is utilized to verify hypothesis, to correlate relationships among multiple data sets, and to identify target data within a large data set. Based on this analysis, the information security analysis system enables the development of resources for management of a network.**

Appellant contends that the nodal diagrams discussed in Maloney at Col. 6, line 64 to Col 7, line 6 are not historical histograms, nor are they the related to the features disclosed by Maloney in Col. 10, lines 37-45. Therefore, Maloney's discussion of: "associations between a number of different charts to determine if such data charts correlate or differentiate." or the discussion "Relationships between an array of data sources is utilized to verify hypothesis, to correlate relationships among multiple data sets, and to identify target data within a large data set." fails to describe "characterizing an attack based on comparison of a historical histogram with the produced histogram data for one or more parameters.

Maloney neither describes that the different charts are used to characterize an attack nor that the different charts are compared with a produced chart (that is, histogram, as claimed) for one or more parameters. In contrast, Maloney describes that: "Based on this analysis, the information security analysis system enables the development of resources for management of a network." Maloney describes Nodal diagrams as: "nodal diagrams thereby permitting an analysis the flexibility to view and observe the interconnections within a large body of code for computer equipment that supports digital data communication networks." [Maloney col. 6, line 4] are not the equivalent of historical histograms.

Claim 7 and by analogy claim 21 are allowable over Maloney since "Anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim." *Connell v. Sears, Roebuck & Co.*, 220 U.S.P.Q. 193, 198 (Fed. Cir. 1983) and Maloney fails to disclose the feature of the histograms and the feature of characterizing an attack based on comparison of a historical histogram with the produced histogram data for one or more parameters.

Claim 22

Regarding Claim 22, Claim 22 limits the monitoring device of claim 21. Appellant contends that Maloney fails to disclose the monitoring device including a process to correlate suspicious parameters to reduce blocking of legitimate traffic. The examiner contends that:

> **Maloney discloses the vector-based correlation process that correlates suspicious parameters and determines existence of correlations of those parameters that can point to types of attacks and reduce dropping legitimate traffic see Col 6 Ln 63-Col 7 Ln 11**

Maloney, Col. 6, line 63 to Col 7, line 6 is the same passage that the examiner used to teach a histogram. However, neither at that passage nor elsewhere does Maloney correlate suspicious parameters to reduce blocking of legitimate traffic. Rather, Maloney only teaches to create associations between a number of different charts to determine if such data charts correlate or differentiate. Among the uses of the cited teachings are to use the relationships between an array of data sources to verify hypothesis, to correlate relationships among multiple data sets, and to identify target data within a large data set. Nowhere does Maloney suggest to "a process to correlate suspicious parameters to reduce blocking of legitimate traffic."

2. Claims 1-6, 18-20, 22, and 28-37 are patentable over U.S. Patent 6,301,668 B1 Gleichauf et al. in view of Maloney.

Claims 1, 3 and 4

For the purposes of this appeal only Claims 1, 3 and 4 stand or fall together. Claim 1 is representative of this group of claims.

Claim 1 recites a process that monitors network traffic through a monitoring device disposed between a data center and a network for thwarting denial of service attacks on the data center. Claim 1 includes the features of a detection process to determine if the values of a parameter of network traffic exceed normal values for the parameter to indicate an attack on the data center and a characterization process to build a histogram for the parameter to compute significant outliers in a parameter and classify the attack. Claim 1 also includes a filtering process for filtering of network packets based on the characterization process.

The examiner contends that:

> **Regarding Claim 1, Gleichauf discloses a detection process to determine to (sic) if the parameter has exceeded normal values see Col 8 Ln 46- Col 9 Ln 3; the filtering process based on the characteristic and being incorporated in a firewall, router, and ID system see Col 1 Ln 22-31 & Col 4 Ln 33-39. Gleichauf does not disclose a process of building an graph to and to classify the attack. However, Maloney discloses the building of graph and the classifying of the attack see Col 10 Ln 37-45. It would be obvious to one having ordinary skill in the art at the time of the invention to include the building of graph and the classifying of the attack in the invention of Gleichauf in order to allow the systems administrator to take appropriate measures as taught in Maloney see Col 7 Ln 40-Col 8 Ln 12. And further, Gleichauf discloses the possibly of visual representation see Fig. 3 item 64, thus the inclusion of a building a graph would be reasonable successful.**

Appellant contends that no combination of Gleichauf with Maloney would suggest the features of claim 1. Gleichauf discloses a vulnerability assessment system. As such, Gleichauf fails to suggest a process that monitors network traffic through a monitoring device disposed between a data center and a network for thwarting denial of service attacks on the data center and a detection process to determine if the values of a parameter exceed normal values for the parameter to indicate an attack on the data center. The examiner contends that Gleichauf teaches this later feature at Col 8, Ln 46-Col 9, Ln 3 and the filtering process based on the characteristic at Col 1, Ln 22-31 & Col 4, Ln 33-39. Appellant disagrees. While Appellant notes that Gleichauf does disclose network security system 20 that comprises

> **a scan engine 22 and a protocol engine 24 coupled to network backbone 14. A signature engine 26 is coupled to protocol engine 24. Scan engine 22 is further coupled to network map 28. Signature engine 26 is coupled to attack signatures 30. A priority engine 32 is coupled to network map 28, protocol engine 24 and signature engine 26. Protocol engine 24 and signature engine 26 each also couple a storage 36. [Gleichauf Co. 4, line 60]**

the examiner has not directed any arguments to that teaching of Gleichauf. Rather, the examiner focusing on the teaching at Col. 8, line 46 to col. 9, line 3, which deals with a vulnerability assessment process not a process to thwart a denial of service attack (See for example col. 7, lines 65-66). Gleichauf whether in col. 8 or elsewhere fails to teach: "a detection process to determine if the values of a parameter for the network traffic exceed normal values for the parameter to indicate an attack on the data center." Rather, (in Col. 8 and Col. 9) Gleichauf discusses protocol analysis 111 and attack signatures 113. Gleichauf discloses that these processes 111 and 113 occur in protocol engine 24 and signature engine 26, at Col. 9, Line 55.

> **Further in operation, protocol engine 24 performs a plurality of protocol analyses upon monitored traffic on network backbone 14 in order to detect attacks upon the network. Attacks upon the network, as mentioned above, are defined herein to include unauthorized accesses, policy violations, and patterns of misuse. Protocol engine 24 can perform, for example, the following protocol analyses upon monitored traffic on network backbone 14: checksum verification (IP, TCP, UDP, ICMP, etc.), IP fragment reassembly, TCP stream reassembly, protocol verification (such as insuring the IP header length is correct and the TCP data gram is not truncated), and timeout calculations.**
>
> **Signature engine 26 is coupled to protocol engine 24 and can perform further analysis tasks in order to detect attacks upon network backbone 14. Signature engine 26 compares monitored traffic with attack signatures 30. Attack signatures 30 can comprise, for example, a rules-based hierarchy of traffic signatures of known policy violations. Signature engine 26 can compare packets from the network traffic with such attack signatures 30 such that policy violations can be discovered.**

Neither of these teachings suggests "a detection process to determine if the values of a parameter for the network traffic exceed normal values for the parameter to indicate an attack on the data center." A signature engine does not determine if values of a parameter exceed normal values for the parameter, but rather seeks to match a signature of an attack to known attack signatures. For instance, Gleichauf discloses: "A signature analysis or pattern matching algorithm is used upon the packets, wherein the packets are compared to "attack signatures", or signatures of known policy violations or patterns of misuse." [Gleichauf, Col. 1, lines 27-31] A protocol engine while performing protocol analysis again does not determine if values of a parameter exceed normal values for the parameter. Rather, the protocol engine performs: "protocol analyses upon monitored traffic on network backbone 14: checksum verification (IP, TCP, UDP, ICMP, etc.), IP fragment reassembly, TCP stream reassembly, protocol verification

(such as insuring the IP header length is correct and the TCP data gram is not truncated), and timeout calculations." [At Col. 9, Lines 50-54].

The examiner relies on Maloney to teach: "a characterization process to build a histogram for the parameter to compute significant outliers in a parameter and classify the attack." As discussed above, Maloney at Col. 10, lines 37-45, describes "a statistical matrix of the data contained in packet and session logs." Maloney also describes the instance of a protocol as the "Y access" and the source IP address as the "X access." Maloney fails to describe or suggest producing a histogram, and in particular fails to suggest computing significant outliers in a parameter and classifying the attack.

Claims 2 and 5

For the purposes of this appeal only Claims 2 and 5 stand or fall together. Claim 2 is representative of this group of claims.

Claim 2 limits the characterization process of claim 1 to include the feature that suspicious parameter values are represented by a bit vector with a 1 in every position corresponding to a "bad" value, and a 0 in every position corresponding to a "good" value.

The examiner acknowledges that Gleichauf fails to disclose this feature and relies on Maloney Col. 6, line 67 to Col. 7, line 11 (reproduced below):

> **Following parsing of the knowledge base 16 the analytical engine 20 responds to the data for preparation and converting into vector-based nodal diagrams. Typically the analytical engine 20 creates associations between a number of different charts to determine if such data charts correlate or differentiate. Relationships between an array of data sources is utilized to verify hypothesis, to correlate relationships among multiple data sets, and to identify target data within a large data set. Based on this analysis, the information security analysis system enables the development of resources for management of a network.**
>
> **The analytical engine 20 analyzes network data to relate knowledge base data to session data, packet data, and alert data as these relationships are utilized to determine who has been talking to whom as well as the content of the traffic for specific protocols.**

Clearly, Maloney does not suggest a bit vector or the feature that suspicious parameter values are represented by a bit vector in this passage or indeed elsewhere. Rather, the vector based nodal diagram disclosed by Maloney is used to: "observe the interconnections within a large body of code for computer equipment that supports digital data communication networks."

The vector based nodal diagram however is not a bit vector. Neither the vector based nodal diagram nor the disclosed use of the diagram suggests the bit vector features of claim 2.

Claim 6

Claim 6 further limits the process of claim 1 to parameters that include at least one of source IP address, destination IP address, source TCP/UDP ports, destination TCP/UDP ports, IP protocol, IP TTL, IP length, hash of payload fragment, IP TOS field, and TCP flags. If values for one or more of these parameters exceed normal values for the parameter a characterization process builds a histogram for the parameter to compute significant outliers in the parameter and classify the attack. Filtering of network packets is performed according to the characterization outcome.

Neither Gleichauf nor Maloney disclose use of these network parameters for construction of a histogram or to compute significant outliners in the parameter.

Claim 18

Claim 18 depends from claim 7, which was rejected by the examiner in view of Maloney alone. Claim 18 recites similar limitations as claim 6 and serves to further distinguish over Gleichauf and Maloney for analogous reasons discussed in claim 6.

Claim 22

The examiner previously rejected claim 22 over Maloney alone and now also rejects this claim over Gleichauf in view of Maloney.

Claim 22 is further limits the device of claim 21 to include a process to correlate suspicious parameters to reduce blocking of legitimate traffic. For all of the reasons discussed above, Maloney fails to disclose this feature. Gleichauf and Maloney together also fail to disclose this feature. The examiner does not offer any reasons why Gleichauf and Maloney together disclose what Maloney alone fails to disclose.

Claim 28

Claim 28 is directed to a computer program product ... including instructions to build a histogram for a parameter of network traffic and use the histogram data for the parameter to characterize an attack. The examiner contends that:

> **19. Regarding Claim 28-31 and 32, Gleichauf discloses a detection process to determine to if (sic) the parameter has exceeded normal values see Col 8 Ln 46-Col 9 Ln 3; the filtering process based on the characteristic and being incorporated in a firewall, router, and ID system see Col 1 Ln 22-31 & Col 4 Ln 33-39. Gleichauf does not disclose a process of building an graph to and to classify the attack. However, Maloney discloses the building of graph and the classifying of the attack see Col 10 Ln 37-45. It would be obvious to one having ordinary skill in the art at the time of the invention to include the building of graph and the classifying of the attack in the invention of Gleichauf in order to allow the systems administrator to take appropriate measures as taught in Maloney see Col 7 Ln 40-Col 8 Ln 12. And further, Gleichauf discloses the possibly of visual representation see Fig. 3 item 64, thus the inclusion of a building a graph would be reasonable successful.**

In formulating this rejection, the examiner urges a combination of Gleichauf with Maloney, but does not use Gleichauf for any feature of claim 28. Rather, the examiner relies solely on Maloney. However, Maloney does not teach a histogram or to "characterize an attack based on the histogram.", as generally argued by Appellant for Claim 1.

Nonetheless, Appellant contends that Gleichauf, like Maloney, does not suggest to use the histogram data for the parameter to characterize an attack. Appellant also contends that Gleichauf fails to disclose characterizing an attack at Col. 8, line 46 to Col. 9, line 3 or elsewhere. Rather, at that passage Gleichauf discloses steps to take in enabling and disabling services running on the security system based on processor utilization. This has nothing at all to do with characterization of an attack.

Therefore, any combination of Gleichauf with Maloney would fail to suggest, claim 28 because neither reference suggests instructions to build a histogram for a parameter of network traffic and instructions to use the histogram data for the parameter to characterize an attack.

Claim 29

Claim 29 serves to further limit claim 28 by including instructions to filter network traffic based on characterization of the attack. Neither reference suggests the characterization recited in claim 28 and therefore neither would suggest to filter based on the characterization.

Claims 30 and 31

For the purposes of this appeal only Claims 30 and 31 stand or fall together. Claim 30 is representative of this group of claims.

Claim 30 further limits the computer program product of claim 28 by reciting instructions to determine if the values of a parameter exceed normal values for the parameter to indicate an attack on the site. The examiner contends that: "Gleichauf discloses a detection process to determine to if (sic) the parameter has exceeded normal values see Col 8 Ln 46- Col 9 Ln 3."

Gleichauf, at Col. 8, line 46 to Col. 9 line 3, discusses prioritization of analysis tasks and system services. Gleichauf determines both memory utilization (at step 117) and processor utilization (at step 119) and overall system bandwidth (at 121) and uses that data along with the criticality of each service to enable or disable tasks to adapt to changing network environments. These teachings however have nothing at all to due with the claimed instructions to determine if the values of a parameter exceed normal values for the parameter to indicate an attack on the site. Recall that claim 30 depends from claim 28, which includes instructions to build a histogram for a parameter of network traffic. The parameter is of network traffic that is used to build the histogram. Neither Gleichauf nor Maloney determine if the values of such a parameter exceed normal values. Neither reference has any concept of a normal value for such a parameter.

Claim 32

Claim 32 is directed to a method of protecting a data center during a denial of service attack. Features of claim 32 include monitoring network traffic through a gateway disposed between the data center and a network, determining if values of at least one parameter exceed normal, threshold values expected for the parameter to indicate an attack on the site, producing a histogram for the at least one parameter of network traffic to characterize the attack by comparing the histogram to at least one historical histogram for that parameter, and filtering out traffic based on characterizing the traffic, which the gateway deems to be part of an attack.

The examiner contends that: "Gleichauf discloses a detection process to determine to if (sic) the parameter has exceeded normal values see Col 8 Ln 46- Col 9 Ln 3; the filtering process based on the characteristic and being incorporated in a firewall, router, and ID system see Col 1 Ln 22-31 & Col 4 Ln 33-39."

Gleichauf does not disclose characterizing an attack at Col. 8, line 46 to Col. 9, line 3 or elsewhere. Rather, at that passage Gleichauf discloses steps to take in enabling and disabling services running on the security system based on processor utilization. This has nothing at all to do with characterization of an attack. Although not specifically mentioned in the examiner's action, it is possible that the examiner contends that the parameter recited in Claim 32 corresponds to processor utilization disclosed in Gleichauf. However, claim 32 requires monitoring network traffic ... and determining if values of at least one parameter exceed normal, threshold values expected for the parameter to indicate an attack on the site. There is no indication in Gleichauf whether processor utilization has any connection with an indication of an attack on a site.

Claim 32 of course requires more, namely, "producing a histogram for the at least one parameter of network traffic to characterize the attack ... " Therefore, recited in claim 32 is the additional limitation that the parameter is that of network traffic. Process utilization is not a parameter of network traffic.

The examiner admits that Gleichauf fails to disclose producing a histogram or comparing the histogram to at least one historical histogram for that parameter. Specifically, the examiner contends that: "Gleichauf does not disclose a process of building an (sic) graph to and to classify the attack. However, Maloney discloses the building of graph and the classifying of the attack see Col 10 Ln 37-45." As Appellant has already discussed, Maloney does not teach a histogram, and does not teach to apply the histogram to characterize an attack. Indeed, while Maloney discloses a graph, that graph is not a histogram, but rather is a statistical matrix of the data contained in packet and session logs. [Maloney, Col. 10, lines 39-40]. Maloney however states that: "the KB summation tool screens the appropriate log file and displays available access criteria to create a graph." In rejection of claim 32 the examiner does not even refer to the teaching of Maloney at Col. 6, line 64 to Col 7, line 6 relied on earlier for support for characterization.

Nevertheless, the nodal diagrams discussed in Maloney at Col. 6, line 64 to Col 7, line 6 are neither historical histograms nor are they the same entities disclosed by Maloney in Col. 10, lines 37-45 and therefore are not used in characterization.

The examiner contends that: "It would be obvious to one having ordinary skill in the art at the time of the invention to include the building of graph and the classifying of the attack in the invention of Gleichauf in order to allow the systems administrator to take appropriate measures as taught in Maloney see Col 7 Ln 40-Col 8 Ln 12. And further, Gleichauf discloses the possibly of visual representation see Fig. 3 item 64, thus the inclusion of a building a graph would be reasonable successful."

Appellant contends that the motivation advanced by the examiner to combine Gleichauf with Maloney is inadequate. The motivation identified in Maloney is related to construction of the nodal diagram. However, according to Maloney: "Nodes are sources of computer traffic, and include servers and host and clients." Therefore, combining Maloney with Gleichauf would permit Gleichauf to display a nodal map of the network for the disclosed vulnerability assessment tool. However, the purported combination would still not motivate one of ordinary skill to provide the features of claim 32 including ... determining if values of at least one parameter exceed normal, threshold values expected for the parameter to indicate an attack on the site; producing a histogram for the at least one parameter of network traffic to characterize the attack by comparing the histogram to at least one historical histogram for that parameter, and filtering out traffic based on characterizing the traffic, which the gateway deems to be part of an attack."

Claims 33, 34, 35 and 36

For the purposes of this appeal only claims 33, 34, 35 and 36 stand or fall together. Claim 33 is representative of this group of claims.

Claim 33 serves to further distinguish over Gleichauf with Maloney. Claim 33 includes the feature of communicating statistics collected in the gateway to a control center. Recall that, claim 32 includes the feature of monitoring network traffic through a gateway disposed between the data center and a network. The examiner contends that: "Regarding Claim 33, 34, 35, and 36, Gleichauf discloses the communicating statistics to a control center, the gateway being deployed in the network and filtering occurs on nearby routers see Fig.1 item 5, Fig. 2 item 20, Fig. 2 item 16 and 32."

Claim 33 distinguishes over Gleichauf with Maloney because no combination of those references discloses the feature of communicating statistics collected in the gateway to a control center. Fig.1 item 5 in Gleichauf is merely a block in a flow diagram. Fig. 2 item 20 is a network security system 20, which includes scan engine. Fig. 2 items 16 and 32 are a firewall, router and a protocol engine (which is also part of the network security system).

In contrast, Gleichauf at Col. 4, line 52 discloses that: Router 18 serves as a gateway between internal network 10 and an external network 30. Gleichauf at Col. 4, line 58, also discloses that: "Internal network 10 further comprises network security system 20 coupled to network backbone 14. Network security system 20 comprises a scan engine 22 and a priority engine 24 coupled to network backbone 14."

It would appear from the way that Gleichauf describes the system that the router 18 does not collect statistical information, (statistical information is not mentioned in Gleichauf) and Gleichauf does not disclose communication of statistics collected in the router 18 to the network security system 20. Rather, according to Gleichauf: "the scan engine 22 gathers the network information" [Gleichauf Col. 4, line 49]. Therefore since the scan engine 22 is in the unit 20 identified by the examiner, Gleichauf fails to disclose "communicating statistics collected in the gateway to a control center," since as in claim 33.

Claim 37

Claim 37 is distinguished over Gleichauf with Maloney. Claim 37 recites the features of ... producing a histogram of network traffic to characterize an attack and filtering out traffic deemed part of an attack, which are neither described nor suggested by any combination of Gleichauf with Maloney. Claim 37 also includes features of the claimed filtering. In claim 37, filtering includes constructing a master correlation vector having asserted bits corresponding to the most important parameter correlations and initializing a packet's correlation bit vector to 0. For every parameter, the claim requires retrieving the parameter in a parameter suspicious vector to construct the packet's correlation bit vector and using the value of the packet's correlation bit vector to index into the master correlation bit vector. The examiner argues in part that:

Gleichauf does not disclose a vector-based correlation process that correlates suspicious parameters and determines existence of correlations of those

> **parameters that can point to types of attacks and reduce dropping legitimate traffic . However, Maloney discloses the vector-based correlation process that correlates suspicious parameters and determines existence of correlations of those parameters that can point to types of attacks and reduce dropping legitimate traffic see Col 6 Ln 63 to Col 7 Ln 11. It would be obvious to one having ordinary skill in the art at the time of the invention to include a correlation process that correlates suspicious parameters and determines existence of correlations of those parameters that can point to types of attacks in the invention of Gleichauf in order to a precise relationship and to differentiate between legitimate traffic as taught in Maloney see Col 7 Ln 7-11.**

Maloney, whether in the cited passages or elsewhere, fails to disclose any filtering that uses a master correlation vector having asserted bits corresponding to the most important parameter correlations and packet correlation bit vectors. What Maloney discloses at Col. 6, lines 63 to Col. 7, line 11, is:

> **Following parsing of the knowledge base 16 the analytical engine 20 responds to the data for preparation and converting into vector-based nodal diagrams. Typically the analytical engine 20 creates associations between a number of different charts to determine if such data charts correlate or differentiate. Relationships between an array of data sources is utilized to verify hypothesis, to correlate relationships among multiple data sets, and to identify target data within a large data set. Based on this analysis, the information security analysis system enables the development of resources for management of a network.**
>
> **The analytical engine 20 analyzes network data to relate knowledge base data to session data, packet data, and alert data as these relationships are utilized to determine who has been talking to whom as well as the content of the traffic for specific protocols.**
>
> **In the process of analyzing network data received by the discovery tool 12 (discovery engine) a determination must also be made as to what communication exist in more than one data set. Characterizing the data in this way utilizes taking a periodic snapshot of captured data over a time period. Averages are then made of what relationships exist to create a link chart representing traffic between data sets.**

Thus, not only is this passage devoid of any discussion of filtering using a master correlation vector having asserted bits corresponding to the most important parameter correlations and packet correlation bit vectors, this passage does not even discuss filtering.

Claim 38

Claim 38 is allowable over the combination of references since no combination suggests testing the indexed bit in the master correlation vector, where if the bit in the master correlation bit vector is a one, the packet is dropped, otherwise the packet is forwarded.

As discussed above for claim 37, no combination of Gleichauf and Maloney discloses a master correlation bit vector. Therefore, no combination of Gleichauf and Maloney could disclose testing of the indexed bit in the master correlation vector and specifically use that technique for dropping or forwarding a packet.

Conclusion

Appellant submits that Claims 7, 21, and 22 are not anticipated under 35 U.S.C. 102(e) by U.S. Patent 6,304,262 by Maloney et al. and claims 1-6, 18-20, 22, and 28-37 are not obvious 35 U.S.C. 103(a) over U.S. Patent 6,301,668 B1 Gleichauf et al. in view of Maloney. Therefore, the Examiner erred in rejecting Appellant's claims and should be reversed.

Respectfully submitted,

Date: 5/23/06

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110-2804
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21312648.doc

Appendix of Claims

1. A process that monitors network traffic through a monitoring device disposed between a data center and a network for thwarting denial of service attacks on the data center, the process comprises:

a detection process to determine if the values of a parameter of network traffic exceed normal values for the parameter to indicate an attack on the data center;

a characterization process to build a histogram for the parameter to compute significant outliers in a parameter and classify the attack; and

a filtering process for filtering of network packets based on the characterization process.

2. The process of claim 1 wherein, in the characterization process, suspicious parameter values are represented by a bit vector with a 1 in every position corresponding to a "bad" value, and a 0 in every position corresponding to a "good" value.

3. The process of claim 1 wherein the characterization process comprises:

a correlation process that correlates suspicious parameters and determines existence of correlations of those parameters that indicate types of attacks.

4. The process of claim 3 wherein the correlation process is used to reduce dropping of legitimate traffic.

5. The process of claim 2 wherein filtering is aggregate filtering.

6 The process of claim 1 wherein parameters include at least one of source IP address, destination IP address, source TCP/UDP ports, destination TCP/UDP ports, IP protocol, IP TTL, IP length, hash of payload fragment, IP TOS field, and TCP flags.

7. A method for thwarting denial of service attacks on a data center, the method comprising:

producing a histogram of received network traffic for at least one parameter of network packets; and

characterizing an attack based on comparison of a historical histogram with the produced histogram data for one or more parameters.

Claims 8-17 were objected to as being dependent on a rejected base claim, but would be allowable if re-written in independent form including the limitation of the base claim and any intervening claims

18. The method of claim 7 wherein attributes include at least one of source IP address, destination IP address, source TCP/UDP ports, destination TCP/UDP ports, IP protocol, IP TTL, IP length, hash of payload fragment, IP TOS field, and TCP flags.

19. The method of claim 7 wherein the method is executed on a data collector.

20. The method of claim 7 wherein the method is executed on a gateway.

21. A monitoring device for thwarting denial of service attacks on a data center, the monitoring device comprises:

a computing device executing:

a process to build at least one histogram for at least one parameter of network traffic; and

a process to characterize an attack based on a comparison of a historical histogram of the at least one parameter to the built at least one histogram for the at least one parameter.

Claims 22-24 were objected to as being dependent on a rejected base claim, but would be allowable if re-written in independent form including the limitation of the base claim and any intervening claims

25. The monitoring device of claim 21 wherein the device is a gateway device that is adaptable to dynamically install filters on nearby routers.

26. The monitoring device of claim 21 wherein the device is a data collector.

27. The monitoring device of claim 21 wherein the parameters include at least one of source IP address, destination IP address, source TCP/UDP ports, destination TCP/UDP ports, IP protocol, IP TTL, IP length, hash of payload fragment, IP TOS field, and TCP flags.

28. A computer program product residing on a computer readable medium comprising instructions for causing a processor to:

build a histogram for a parameter of network traffic; and

use the histogram data for the parameter to characterize an attack.

29. The computer program product of claim 28 further comprising instructions to:

filter network traffic based on characterization of the attack.

30. The computer program product of claim 28 further comprising instructions to:

determine if the values of a parameter exceed normal values for the parameter to indicate an attack on the site;

31. The computer program product of claim 30 further comprising instructions to:

use the histogram to characterize the attack when it is determined that one of the parameters exceeds a threshold.

32. A method of protecting a data center during a denial of service attack, the method comprises:

monitoring network traffic through a gateway disposed between the data center and a network:

determining if values of at least one parameter exceed normal, threshold values expected for the parameter to indicate an attack on the site;

producing a histogram for the at least one parameter of network traffic to characterize the attack by comparing the histogram to at least one historical histogram for that parameter; and

filtering out traffic based on characterizing the traffic, which the gateway deems to be part of an attack.

33. The method of claim 32 further comprising:

communicating statistics collected in the gateway to a control center.

34. The method of claim 33 wherein communicating occurs over a dedicated link to the control center via a hardened network.

35. The method of claim 33 wherein the gateway is physically deployed in line in the network.

36. The method of claim 33 wherein filtering occurs on nearby routers.

37. A method to reduce blocking of legitimate traffic in a process to protect a victim site during a denial of service attack, comprises:

producing a histogram of network traffic to characterize an attack; and

filtering out traffic deemed part of an attack with filtering comprising:

constructing a master correlation vector having asserted bits corresponding to the most important parameter correlations;

initializing a packet's correlation bit vector to 0, and for every parameter:

retrieving the parameter in a parameter suspicious vector to construct the packet' correlation bit vector; and

using the value of the packet's correlation bit vector to index into the master correlation bit vector.

38. The method of claim 37 further comprising:

testing the indexed bit in the master correlation vector, where if the bit in the master correlation bit vector is a one, the packet is dropped, otherwise the packet is forwarded.

Claims 39 and 40 were objected to as being dependent on a rejected base claim, but would be allowable if re-written in independent form including the limitation of the base claim and any intervening claims

Evidence Appendix

None

Related Proceedings Appendix

None